IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

APPLICANT: Narayanaswami et al. EXAMINER: Rashawn N. Tillery

SERIAL NO.: 09/080,517 GROUP ART UNIT: 2612

FILED: May 18, 1998 Docket: YO998-095 (8728-118)

FOR: AN IMAGE CAPTURING SYSTEM AND METHOD FOR AUTOMATICALLY WATERMARKING RECORDED PARAMETERS FOR PROVIDING DIGITAL IMAGE VERIFICATION

Mail Stop: Appeal Brief Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF

Sir:

Enclosed please find APPELLANTS' APPEAL BRIEF in triplicate.

Please charge Deposit Account No. 50-0510/IBM(Yorktown Heights) in the amount of $330.00 to cover the appeal fee. Please charge any deficiency as well as any other fee(s) which may become due under 37 C.F.R. § 1.16 and/or 1.17, at any time during the pendency of this application, or credit any overpayment of such fee(s), to Deposit Account No. 50-0510/IBM (Yorktown Heights). **TWO (2) COPIES OF THIS SHEET ARE ENCLOSED.**

Respectfully submitted,

Frank V. DeRosa
Reg. No. 43,584
Attorney for Applicant(s)

F. CHAU & ASSOCIATES, LLP
1900 Hempstead Turnpike, Suite 501
East Meadow, NY 11554
Tel: (516) 357-0091
Fax: (516) 357-0092

CERTIFICATE OF MAILING UNDER 37 C.F.R. §1.8(a)

I hereby certify that this correspondence and accompanying documents are being deposited with the United States Postal Service as first class mail, postpaid in an envelope, addressed to the: Mail Stop Appeal Brief Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on February 19, 2004.

Dated: February 19, 2004

Frank V. DeRosa

PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Applicants: Narayanaswami et al.	**Examiner:** Rashawn N. Tillery
Serial No.: 09/080,517	**Group Art Unit:** 2612
Filed: May 18, 1998	**Docket:** 8728-118 (YO998-095)

For: **An Image Capturing System And Method For Automatically Watermarking Recorded Parameters For Providing Digital Image Verification**

APPEAL BRIEF

Appeal from Group 2612

F. Chau & Associates, LLC
1900 Hempstead Turnpike
East Meadow, New York 11554
TEL: (516) 357-0091
FAX: (516) 357-0092
Attorneys for Appellant

TABLE OF CONTENTS **Page(s)**

I. INTRODUCTION

This Appeal is from a Final Office Action mailed on July 1, 2003 (Paper No. 15) (hereinafter, referred to as the "Final Action") finally rejecting claims 1-22 of the above-identified application, and an Advisory Action mailed on October 17, 2003 (Paper No. 17). Applicants commenced this Appeal by a Notice of Appeal filed on November 19, 2003, and hereby submit this Appeal Brief.

II. REAL PARTY IN INTEREST

The real party in interest for the above-identified application is International Business Machines (IBM) Corporation, the assignee of the entire right, title and interest in and to the subject application by virtue of an assignment of record in the U.S. Patent and Trademark Office.

III. RELATED APPEALS AND INTERFERENCES

There are no Appeals or Interferences known to Applicant, Applicant's representatives or the Assignee, which would directly affect or be indirectly affected by or have a bearing on the Board's decision in the pending Appeal.

IV. STATUS OF CLAIMS

Claims 1-22 are pending, stand rejected and are under appeal. The claims on appeal are set forth in the attached Appendix.

Claims 1, 13 and 18 are independent claims. Claims 2-12 depend directly or indirectly from claim 1. Claims 14-17 and 21 depend directly or indirectly from claim 13. Claims 19-20 and 22 depend directly or indirectly from claim 18.

V. STATUS OF AMENDMENTS

No after final Amendments were filed in this case subsequent to the Final Action.

VI. SUMMARY OF THE INVENTION

In general, the claimed inventions are directed to systems and methods for verifying the authenticity of digital images. Systems and methods according to the invention for providing verification include watermarking process for watermarking one or more recorded camera/image parameters within a captured image, wherein the recorded parameters are associated with the captured image, and extracting the watermarked parameters for purposes of authentication.

More specifically, an image capturing system according to the invention employs methods for automatically recording one or more camera/image parameters associated with a captured image, and automatically watermarking the recorded camera/image parameter(s) within the captured image. The watermarking process is used to invisibly watermark (i.e., hide) one or more of the recorded parameters within the captured image. The original recorded parameters associated with the captured image are stored for subsequent access. For example, the parameters can be stored in an image header of the captured image and/or in a separate file associated with the captured image.

The camera/image parameters that can be automatically recorded with a captured image include, for example, names of geographic locations, altitude, longitude, time, date, photographer identification, as well as image data such as light intensity, shutter speed and flash status, etc.

The authenticity of the digital (captured) image can subsequently be verified by extracting the watermarked parameters from the capture image, and then comparing the extracted parameters with the original recorded parameters to determine whether the recorded parameters match the extracted parameters. Since the recorded parameters are watermarked into the image, it is difficult to modify the image without affecting the watermarked data. Therefore, if the extracted data appears corrupted (the extracted parameters does not match the recorded parameters associated with the image), it is an indication that the image is not authentic and has been modified or otherwise tampered with.

Furthermore, since the recorded parameters are watermarked into the image, a mismatch between the extracted parameters and the original recorded parameters (which are, e.g., recorded in the image header) is an indication that one or more of the originally recorded parameters are not authentic, e.g., have been modified or otherwise tampered with. More specifically, systems and methods according to the invention which automatically watermark (i.e., hide) a plurality of recorded parameters into each image are useful for verifying and confirming the circumstances and conditions surrounding the capturing of the digital image.

For instance, recording and watermarking parameters, which are associated with a captured image, such as such as names of geographic locations, altitude, longitude, time, date, photographer identification, as well as image data such as light intensity, shutter speed and flash status, would be very useful to, e.g., insurance agencies, to determine and verify the conditions and circumstances (such as time, date, and location) in connection with the capturing of an image. For instance, such information can be of immense value to insurance agencies (e.g., real-estate, auto, and fire), hospitals, news agencies and crime investigating agencies, for confirming the details surrounding an accident so as to assist in the investigation of the accident and preparing the necessary accident reports.

The inventions of independent claims 1, 13 and 18 broadly embody features of the claimed inventions as discussed above, for example.

Claim 1 is directed to an image capturing system for automatically recording and watermarking a plurality of parameters in a captured image, comprising, inter alia:

wireless communication means, operatively connected to said central processing unit, for receiving object data from objects in said observed image frame when said image is generated, said object data comprising object identification information;

information receiving means, operatively coupled to said central processing unit, for receiving user data associated with a user of said system when said digital image is generated, said user data comprising user identification information;

image processing means for receiving said plurality of parameters and recording said plurality of parameters with said generated digital image, said plurality of parameters including . . . said object data, . . . said user data; and

means, operatively coupled to said image processing means, for watermarking said plurality of parameters into said image.

For purposes of illustration, the invention of claim 1 will be further discussed hereafter with reference to the exemplary embodiment depicted in Figure 1, and corresponding description, of Applicants' specification (hereinafter, "Spec."), but nothing herein shall be construed as placing any limitation on the claimed inventions. By way of example, FIG. 1 depicts an image capturing system (100) having a smart card reader (110), a Pan (Personal Area Network) receiver (122), an IR processor (118) or an RF processor (112), which can be used to obtain and record *user data comprising user identification information* such as the identity of the photographer (see, e.g., page 9, lines 3-22, of Spec.). The IR processor (118) or RF processor (112) can be used for communicating with objects being photographed so as to obtain and record *object data comprising object identification information* such as the name and identity of the object being photographed (see, e.g., page 9, line 23, through page 10, line 6). These parameters, e.g., *object identification data* and *user identification data* are recorded with the digital mage and watermarked into the image.

Claim 13 is directed to a method for authenticating a captured image. The claimed method includes measuring a plurality of parameters associated with a captured image and watermarking the plurality of parameters into the captured image to generate a watermarked image. A verification key is generated, which is associated with the watermarked parameters. For authenticating the captured image, the plurality of parameters are extracted from the watermarked image using the associated verification key, and the extracted parameters are compared with the measured plurality of parameters associated with the captured image. The captured image is authenticated if the extracted parameters match the measured parameters.

Claim 18 is directed to a method for verifying the authenticity of a captured image. The method includes a user specifying one or more parameters (e.g., date, time, etc.) that are to be measured and watermarked by an image capturing system. An image is captured of a desired object using the image capturing system. The captured image is watermarked with the specified parameters and a corresponding verification key is generated based on the watermarked parameters. The watermarked image and corresponding verification key are stored. For purposes of authentication, the watermarked image and corresponding verification key an be retrieved from storage, and the watermarked parameters are extracted from the watermarked image using the verification key. The extracted parameters are compared with the specified measured parameters to determine if the extracted parameters match the specified parameters.

VII. ISSUES

(1) Claims 1-8 and 12-22 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,499,294 to Friedman in view of U.S. Patent No. 6,192,138 to Yamadaji.

Thus, one issue on appeal is whether the combination of Yamadaji and Friedman is legally sufficient to establish a *prima facie* case of obviousness against claims 1-8 and 12-22.

(2) Claim 9 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Friedman in view of Yamadaji in further view of U.S. Patent No. 5,799,082 to Murphy et al.

Thus, another issue on appeal is whether the combination of Yamadaji , Friedman and Murphy is legally sufficient to establish a *prima facie* case of obviousness against claim 9.

(3) Claims 10-11 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Friedman in view of Yamadaji in further view of U.S. Patent No. 5,335,072 to Tanaka et al.

Thus, another issue on appeal is whether the combination of Yamadaji, Friedman and Tanaka is legally sufficient to establish a *prima facie* case of obviousness against claims 10 and 11.

VIII. GROUPING OF CLAIMS

For Issue (1) above:

(i) Claims 7, 8 and 12 stand or fall with Claim 1, but claims 2, 3, 4, 5 and 6 are separately patentable and do not fall with Claim 1;

(ii) Claims 16 and 17 stand or fall with Claim 13, but Claims 14, 15 and 21 are separately patentable and do not fall with Claim 13;

(iii) Claims 19 and 22 are separately patentable and do not fall with Claim 18. Claim 20 stands or falls with claim 29.

For Issue (2) above:

Claim 9 stands or falls with Claim 1.

For Issue (3) above:

(i) Claims 10 and 11 stand or fall with Claim 1.

IX. ARGUMENTS

A. The Combination of Friedman and Yamadaji is *Legally Deficient* to Support a *Prima Facie* Case Of Obviousness Against Claims 1, 13 or 18

In rejecting claims under 35 U.S.C. 103, the Examiner bears the initial burden of presenting a prima facie case of obviousness. In re Rijckaert, 9 F.3d 1531, 1532 (Fed. Cir. 1993). The burden of presenting a prima facie case of obviousness is only satisfied by showing some objective teaching in the prior art or that knowledge generally available to one of ordinary skill in the art would lead that individual to combine the relevant teachings of the references. In re Fine, 837 F.2d 1071, 1074 (Fed. Cir. 1988). A prima facie case of obviousness is established when the teachings of the prior art itself would appear to have suggested the claimed subject matter to one of ordinary skill in the art. In re Bell, 991 F.2d 781, 782 (Fed. Cir. 1993). The suggestion to combine the references should come from the prior art, and the Examiner cannot use hindsight gleaned from the invention itself to pick and choose among related disclosures in the prior art to arrive at the claimed invention. In re Fine, 837 F.2d at 1075. If the Examiner fails to establish a prima facie case, the rejection is improper and must be overturned. In re Rijckaert, 9 F.3d at 1532 (citing In re Fine, 837 F.2d at 1074).

In the case at bar, the obviousness rejections of claims 1-22 as set forth in the Final Action are based entirely, or primarily in part, on the combined teachings of Friedman and Yamadaji (see, Section VII, A-C, above). Applicants respectfully submit, however, that at the very minimum, the combination of Friedman and Yamadaji is legally deficient to support a *prima facie* case of obviousness against the inventions of independent claims 1, 13 and 18. For example, as explained below, the Examiner's express acknowledgment of the difference between the combined teachings of Friedman and Yamadaji and the claimed inventions is a clear indication of the impropriety of the obviousness rejections. Moreover, there is no legally sufficient basis for combining the teachings of Friedman and Yamadaji in the manner suggested by the Examiner to support the obviousness rejections. The following discussion will begin with a brief description of Friedman and Yamadaji and Examiner's basis for combining Friedman and Yamadaji, followed by an explanation as to the *impropriety* of the obviousness rejections based on such combination.

In general, Friedman is directed to a digital camera having a processing architecture that enables authentication of a digital image using a "digital signature" scheme based on "public key encryption", which is well known in the art. In particular, Friedman discloses a camera having a processor that is equipped by the manufacture with an embedded "private key" that is unique to the camera. The camera processor includes means for computing an "*image hash*" of an image file (using a predetermined hash function) and means for encrypting the "*image hash*" using the "private key" to thereby generate a "digital signature". The image file and corresponding digital signature are separate entities that are stored together, and the digital signature is used for authenticating the image file.

More specifically, with the Friedman system, authentication of the image file as being free of alteration or modification includes accessing the stored image file and corresponding digital signature and computing an "image hash" of the accessed image file using same predetermined hash function that was used to generate the original image hash. The corresponding digital signature is decrypted using a "public key" to recover the original image hash. Thereafter, the original image hash will be compared to the currently computed image hash. If the original image hash matches the current image hash, the accessed image file is deemed authentic (see, e.g., Friedman, Abstract; and Col. 4, lines 19-54).

Friedman further discloses certain information (e.g., date, time, etc.) may be added in a border region of an image file, which surround the digital image, wherein the added information in the border region can be hashed and encrypted together with the image to generate a digital signature (see, e.g., Col. 4, lines 55-66). Although Friedman discloses that such parameters in the image border are part of the image file that is used for computing and encrypting an image hash to generate a digital signature, these parameters are not necessary for the authentication because the digital signature can be generated by encrypting an image hash of an image file that contains the image alone, wherein authentication is based on matching hashes (see, e.g., Col. 5, line 49, through Col. 6, line 52).

Yamadaji discloses a method for watermarking copyright information (images or textual) in an image for purposes of copyright protection of the image. The copyright data is stored in memory as a digital watermark and the digital watermark can be accessed and embedded within a captured image (see, e.g., Col. 8, line 12 – Col. 9, line 22).

The Examiner's basis of obviousness in view of the combination of Friedman and Yamadaji can be readily gleaned from statements set forth in the Final Action and the Advisory Action (Paper No. 18). For example, although Examiner essentially acknowledges that neither Friedman nor Yamadaji explicitly teach *watermarking a plurality of parameters into an image*, the Examiner contends (on Page 2 of the Final Action) that *"given Yamadaji's teachings of watermarking textual data for purposes of security, that it would have not have been a huge leap for one or ordinary skill in the art to watermark Friedman's parameters into the border of the image."* Furthermore, the Examiner asserts (on Page 3 of the Advisory Action) that "... *the Office acknowledges the difference in Applicant's claimed invention and the prior art – specifically that the combination of Friedman and Yamadaji teaches watermarking parameters in the border of a captured image while Applicant watermarks the captured image of the object with parameters – however the office is unable to ascertain the unexpected result of the difference from a legal standpoint. In other words, both methods of watermarking the parameters yield the same result."* (See, Advisory Action, Page 3.). It is respectfully submitted that Examiner's basis of obviousness as outlined above is legally deficient for various reasons.

(i) The Examiner's Admitted Difference Between the Combined Teachings of Friedman and Yamadaji and the Claimed Inventions is a *Prima Facie* Indication as to the Impropriety of the Obviousness Rejections

Applicants respectfully submit that on a fundamental level, the obviousness rejections of claims 1, 13 and 18 (and all claims that depend there from) are legally deficient on their face at least by virtue of Examiner's acknowledgments that combination of Friedman and Yamadaji does not disclose or suggest every element of the claimed inventions, namely, that such combination does not teach watermarking recorded parameters into a captured image.

Indeed, Examiner's contention that "*it would have not have been a huge leap for one of ordinary skill in the art to watermark Friedman's parameters into the border of the image*" is essentially irrelevant because it does not specifically address the claimed inventions. Indeed, the claimed inventions recite that the parameters are watermarked into an image, not a border of the image. In other words, in the claimed inventions, one or more parameters are hidden (watermarked) within the captured image to, e.g., enable authentication of the image.

In fact, as noted above, the Examiner even acknowledges that a difference between the claimed inventions and the combination of Friedman and Yamadaji is that such combination teaches watermarking parameters in the border of a captured image, whereas the claimed inventions watermark the captured image of the object with parameters. The Examiner's express acknowledgement of the difference between the prior art and the claimed inventions is a *prima facie* indication of the impropriety of the obviousness rejections. Indeed, Examiner essentially admits that the combination of Friedman and Yamadaji fails to disclose or suggest every feature of the claimed invention, such as *watermarking a plurality of parameters into an image*, which renders the obviousness rejections as *prima facie* improper.

(ii) There is No Legally Sufficient Basis for Combining the Teachings of Friedman and Yamadaji to Support the Obviousness Rejections

Although the Examiner acknowledges the "difference" between the prior art and the claimed inventions, as noted above, the Examiner appears to justify the proposed combination of Friedman and Yamadaji on the grounds that there is "no unexpected result of the difference from a legal standpoint" because the method of watermarking the parameters into an image and the method of watermarking the parameters into a border of the image "yield the same result".

It is to be noted that this justification or basis for combining of Friedman and Yamadaji is legally deficient in that it is based essentially on an unsupported and contradictory assertion regarding the "similarity" of what Examiner acknowledges is a "difference" between the claimed inventions and the cited art. The Examiner fails to explain how the admitted "difference" between the claimed inventions and the cited art are "similar."

It is respectfully submitted, however, that there is *no* reasonable basis for this conclusion and that other than through impermissible hindsight reasoning, there is *no* legally sufficient basis or motivation that would lead one of ordinary skill in the art to combine the relevant teachings of the Friedman and Yamadaji in the manner suggested by the Examiner. In particular, it is respectfully submitted that Examiner's basis for obviousness grounded on that "*it would have not have been a huge leap for one or ordinary skill in the art to watermark Friedman's parameters into the border of the image*" is based on impermissible hindsight reasoning in view of Applicants' disclosure since Examiner has **not** explained how one of ordinary skill in the art would not be motivated to combine the teachings of Friedman and Yamadaji in the manner suggest by Examiner for *watermarking Friedman's parameters into the border of the image* .

To begin, although Friedman discloses that information (e.g., time or date) can be captured in the border region of a photograph (see, e.g., Fig. 4 of Friedman), Friedman does not even remotely suggest that such information can be watermarked or otherwise hidden in the image border region. In fact, in stark contrast, Friedman teaches that the information in the border of the image can used by an investigator for identifying and interpreting information by what is depicted in the photograph (see, e.g.., Col. 9, lines For this purpose, it would make no sense in the Friedman system to encrypt or otherwise hide such information in the border region of an image. This is even more evident given the fact that Friedman implements a public/private key protocol for generating a digital signature from an image file, wherein the digital signature is used to authenticate the image. In other words, Friedman does not care about hiding or encrypting parameters within a border of the image, much less the image itself, because authentication is based solely on the separate digital signature that is derived by hashing the image file and encrypting the hash image.

More specifically, as explained above, the claimed inventions provide authentication by watermarking (hiding) captured image parameters into the image itself. With the claimed inventions, it is the watermarked parameters that are actually used for authentication and the captured image itself contains the information (watermarked parameters) for authenticating the image. On the other hand, as explained above, Friedman discloses an image authentication system which implements a public/private key protocol for generating a digital signature from an image file, wherein the digital signature is used to authenticate the image.

In this regard, the authentication protocols of the claimed inventions and of Friedman are very distinct on various levels, that one of ordinary skill in the art would not be motivated to combine watermarking as taught by Yamadaji with the Friedman system to derive a watermarking authentication protocol of the claimed inventions. For instance, the Friedman method utilizes two separate entities, the image file and the corresponding digital signature, for authentication. In contrast, with the claimed inventions, the image file itself (single file) contains information that can be extracted to authenticate the image.

Furthermore, in contrast to the claimed inventions, as explained above, Friedman does not use recorded parameters, *per se*, for purposes of authentication, because the Friedman system can compute a hash of the image file and encrypt the image hash to generate the digital signature regardless of whether or not the image file has a image border region with captured information. In Friedman, the parameters in the image file border are not used, *per se*, to authenticate and image, but rather if such parameters are included in the border region of the image file, the credibility of such recorded data can be upheld if the image file is authenticated via comparison of the computed image hashes (see, e.g., Col. 10, lines 24-26). More specifically, although Friedman discloses a method for verifying the authenticity of an image and that certain parameters associated with a captured image can be recorded in an image border, the Friedman protocol does ***not*** rely on such recorded parameters for authentication. In contrast, Friedman provides image authentication using the well-known digital signature method by calculating a hash of the image and comparing the calculated hash with a secure hash of the digital signature. If the computed hash and secure hash are the same, then the image is deemed authentic. Friedman merely discloses that the credibility of the textual data in the border is upheld during the authentication. But Friedman does not explicitly use the recorded parameters to authenticate the image *vis-à-vis* the digital signature method. In other words, the Friedman authentication protocol can be used for authentication regardless of whether or not recorded parameters are contained in the border of the image.

Moreover, given the fact that Friedman uses a digital signature method for authentication, although Yamadaji discloses the use of watermarking copyright information (images or textual) in an image for purposes of copyright protection of the image, Examiner has failed to show motivation for modifying the teachings of Friedman with the watermarking teachings of Yamadaji and Friedman for using watermarked recorded camera parameters as an authentication protocol. In particular, it is axiomatic that if a proposed modification would render a prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification. See, MPEP 2143.01, citing *In re Gordon*, 733 F.2d 900 (Fed. Cir. 1964). Furthermore, if the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims *prima facie* obvious. See, MPEP 2143.01, citing *In re Ratti*, 270 F.2d 810 (CCPA 1959).

Here, by applying the watermarking teachings Yamadaji to the authentication protocol of Friedman, Examiner attempts to essentially dismiss or disregard Friedman's public/private key/ digital signature authentication protocol. As noted above, the claimed watermarking protocols are significantly different than Friedman's authentication protocol and in this regard, Examiner attempts to change the principle of operation of the Friedman protocol with the teachings of Yamadaji. As such, it is clear that the teachings of the Friedman and Yamadaji are not sufficient to render the claims *prima facie* obvious. Accordingly, for at least the above reasons, there is simply no motivation for combining the teachings of Friedman and Yamadaji in the manner suggested by Examiner other than *impermissible hindsight reasoning*.

(iii) The Combination of Friedman and Yamadaji Does Not Disclose or Suggest Various Elements of Claims 1, 13 or 18

Even assuming, arguendo, that the combination of Friedman and Yamadaji is deemed legally proper, it is respectfully submitted that the combination of Friedman and Yamadaji is *legally deficient* to support a *prima facie* case of obviousness against claims 1-22 because at the very minimum, such combination does not disclose or suggest various features of independent claims 1, 13 and 18.

To begin, Applicants reiterate that for at least the reasons given above, the combination of Friedman and Yamadaji does not disclose or suggest a system or method for, e.g., *watermarking a plurality of parameters into a captured image,* as essentially claimed in claims 1, 13 and 18.

Furthermore, with regard to Claim 1, it is respectfully submitted that the combination of Friedman and Yamadaji does not disclose or suggest a system for capturing images, wherein the system comprises *wireless communication means for receiving object data from objects in an observed image frame when the image is generated, wherein the object data comprises object identification information*. Nor does such combination disclose or suggest *information receiving means for receiving user data associated with a user of the system when the digital image is generated, wherein the user data comprises user identification information*.

In the Final Action, Examiner relies on Friedman as disclosing the above features of claim 1. However, it is respectfully submitted that Examiner's reliance on Friedman in this regard is erroneous and glaringly misplaced. Indeed, it is respectfully submitted that Examiner has provided no reasonable basis for interpreting Friedman as disclosing recorded parameters including (a) object identification information and (b) user identification information, as essentially claimed in Claim 1.

In particular, with regard to element (a) above, Examiner relies on Friedman's disclosure of a range finder (13) (such as an acoustic, optical, laser or infrared) to capture range information of prominent objects in a scene (see, Col. 9, lines 42-46), essentially contending that the range information captured by the range finder (13) can be interpreted as *object data that comprises object identification information* (see, e.g., Pages 3-4 of the Final Action). Although Friedman discloses a rangefinder to collect "range information" to determine the distance an object is from the camera, there is simply no reasonable basis for construing such "range information" as being "object identification" as claimed in claim 1. Indeed, the "distance" an object is to a camera is very different from the "identity" of the object.

Furthermore, with regard to element (b) above, Examiner relies on Friedman's disclosure (Col. 3, lines 1-11) of a "serial number" of a camera as being properly construed as *user data that comprises user identification information* (see, e.g., Page 4 of the Final Action). Friedman discloses that *each digital camera possess its own unique private/public key pair, wherein the public key can be placed on the camera's name plate as a "serial number" or recorded in the border region of an image file* (see, e.g., Col. 7, lines 58-64). However, it is unreasonable to construe a camera "serial number" as being *"user identification information" that is associated with the user of the imaging system when the digital image is captured by the user,* as essentially claimed in Claim 1. Indeed, in the Friedman system, the serial number (or public key) is associated with the camera itself, and not with the user of the camera *per se*. In fact, many different users can use the same camera and in such instance, the "serial number" or public key would clearly not provide information regarding the identity of the person using the camera.

Moreover, with respect to Claims 13 and 18, the combination of Friedman and Yamadaji does not disclose or suggest an authentication protocol that includes *extracting parameters from a watermarked image using an associated verification key, comparing the extracted parameters with the original recorded/measured parameters associated with the captured image to* *determine if the extracted parameters match the originally recorded/measured parameters*, as essentially claimed in claims 13 and 18.

In fact, it should be noted that in the Final Action, the Examiner provides no explanation or specific grounds to support of the rejection of Claims 13 and 18, other than reliance on same grounds of rejection of claim 1 and claims 1 and 2, respectively (see, page 6 and 8 of the Final Action). In relying on the grounds for the rejection of claim 1, however, the Examiner has failed to address various elements of claims 13 and 18. For example, Examiner has not explained how the combination of Friedman and Yamadaji teaches or suggest authentication by, e.g., *comparing watermarked parameters, which are extracted from a captured image, with the original parameters associated with the captured image, to determine if the extracted parameters match the original parameters*, as essentially claimed in claims 13 and 18. In any event, given Examiner's acknowledgement that the combination of Friedman and Yamadaji does not teach watermarking parameters into an image (as noted above), it necessarily and logically follows that such combination does not teach or suggest "extracting watermarked parameters from the watermarked image and comparing the extracted parameters with the original parameters" to authenticate the image.

Thus, for at least the above reasons, claims 1, 13 and 18 are believed to be patentable and non-obvious over the combination of Friedman and Yamadaji. In addition, with respect to the rejection of dependent claims 7-8 and 12 (which depend from base claim 1) and claims 16 and 17 (which depend from base claim 13), such claims are patentable and non-obvious over the combination of Friedman and Yamadaji at least for the same reasons given above for respective base claims 1 and 13.

Furthermore, to the extent that claims 9 and 11 (which depend from claim 1) are rejected, in part, on the combination of Friedman and Yamadaji as applied to claim 1, claims 9 and 11 patentable at least for the same reasons given for claim 1.

B. **The Combination of Friedman and Yamadaji Does Not Disclose or Suggest Elements of Claims 2-6, 14-15, 19, and 21-22**

Claims 2-6, 14-15, 19, and 21-22 are patentable and non-obvious over the combination of Friedman and Yamadaji in their own right. For instance, with respect to claims 2 and 3 (and 15, Examiner admits that neither Friedman nor Yamadaji expressly disclose the claimed invention, but Examiner contends, in conclusory manner, that claims 2 and 3 would have been obvious "to allot user more control over the recorded and watermarked data," (see, page 8 of the Final Action). It is respectfully submitted that Examiner's grounds for obviousness in this regard are clearly based on nothing more than impermissible hindsight reasoning, especially given the fact that Examiner relies on no references as teaching the claimed features of claims 2, 3 and 15.

Furthermore, with respect to claim 6, Examiner admits that neither Friedman nor Yamadaji expressly disclose the claimed invention, but Examiner contends, in conclusory manner, that claim 6 would have been obvious to one of ordinary to *prevent the watermarking of an image if the quality of the image is altered above a threshold* (as recited in claim 6) since "it would be a waste of time and money to watermark a damage/unclear image" (see, Page 8 of the Final Action). In the first instance, Examiner's basis for obviousness misses the point, because the claimed invention contemplates preventing watermarking if the watermarking of the parameter into the image would affect the image quality, but not preventing watermarking of a damaged image as interpreted by Examiner. In any event, assuming Examiner's interpretation of claim 6 to be proper, it is respectfully submitted that Examiner's grounds for obviousness in this regard are clearly based on nothing more than impermissible hindsight reasoning.

Moreover, with respect to claims 4-5, 14 and 19, at least the reasons set forth above for claims 13 and 18, Examiner has utterly failed to explain how the combination of Friedman and Yamadaji teaches comparing the extracted parameters with the original recorded/measured parameters associated with the captured image.

Finally, with respect to claims 21 and 22, for at least the same reasons give above for claim 1, Examiner has misconstrued Friedman as disclosing watermarked parameters that include object identification or user identification information.

C. CONCLUSION

Accordingly, for at least the above reasons, it is respectfully requested that the Board reverse all claim rejections under 35 U.S.C. § 103(a).

Respectfully submitted,

Frank DeRosa
Reg. No. 43,584
Attorney for Applicant(s)

F. Chau & Associates, LLC
1900 Hempstead Turnpike
East Meadow, New York 11553
TEL: (516) 357-0091
FAX: (516) 357-0092

APPENDIX A

1. An image capturing system for automatically recording and watermarking a plurality of parameters in a captured image, comprising:

a central processing unit for controlling a plurality of functions and operations of said system;

image capture means, operatively connected to said central processing unit, for generating a digital image of an observed image frame and for generating a plurality of image data associated with said generation of said image;

wireless communication means, operatively connected to said central processing unit, for receiving object data from objects in said observed image frame when said image is generated, said object data comprising object identification information;

geographic location determining means, operatively connected to said central processing unit, for determining geographic coordinates of said system when said digital image is generated;

means for determining a time and a date when said image is generated;

information receiving means, operatively coupled to said central processing unit, for receiving user data associated with a user of said system when said digital image is generated, said user data comprising user identification information;

image processing means for receiving said plurality of parameters and recording said plurality of parameters with said generated digital image, said plurality of parameters including said plurality of image data, said object data, said time data, said date data, said location data, and said user data; and

means, operatively coupled to said image processing means, for watermarking said plurality of parameters into said image.

2. The system of claim 1, further comprising means for specifying which of the plurality of parameters should be recorded with said image and for specifying which of said plurality of parameters should be watermarked in said image.

3. The system of claim 2, further comprising means for determining which of the plurality of parameters are specified to be recorded with said image and for determining which of the plurality of parameters are specified to be watermarked in said image.

4. The system of claim 1, further comprising means for extracting said watermarked parameters from said watermarked image.

5. The system of claim 4, further comprising means for comparing said extracted parameters with corresponding recorded parameters of said image to authenticate said image.

6. The system of claim 1, further comprising means for preventing said watermarking of said images if an image quality of said image is altered above a threshold.

7. The system of claim 1, further comprising image compression means, operatively coupled to said image processing means, for compressing said image.

8. The system of claim 7, wherein said plurality of parameters are watermarked in one of said compressed image and said image.

9. The system of claim 1, further comprising orientation determining means, operatively coupled to said central processing unit, for determining orientation data of said system when said digital image is generated; said orientation data being one of said plurality of parameters.

10. The system of claim 1, further comprising

means for receiving one of verbal data and verbal commands; and

means for processing said one of received verbal data and received verbal command, said processed verbal commands being used to control one of a plurality of function and operations of said system, said processed speech data being one of said plurality of parameters for annotating said digital image.

11. The system of claim 1, further comprising means for determining said location of said system when said geographic location determining means is inoperable.

12. The system of claim 1, wherein said plurality of image data associated with said generation of said image includes one of an image mode, image quality, exposure duration, aperture length, light meter reading, flash status, lens focal length, auto focus distance, frame number, and a combination thereof.

13. In an image capturing system, a method for authenticating a captured image, comprising the steps of:

measuring a plurality of parameters associated with said captured image;

watermarking said plurality of parameters into said captured image to generate a watermarked image, and generating a verification key associated with said watermarked parameters;

extracting said plurality of parameters from said watermarked image with said associated verification key; and

comparing said extracted plurality of parameters from said watermarked image with said measured plurality of parameters associated with said captured image, whereby said captured image is authenticated if said extracted parameters match with said measured parameters.

14. The method of claim 13, further comprising the step of recording said measured plurality of parameters associated with each captured image, said extracted parameters being compared with said recorded parameters to authenticate said captured image.

15. The method of claim 14, further comprising the step of specifying which of said measured plurality of parameters is to be watermarked into a corresponding captured image.

16. The method of claim 14, further including the step of transmitting said watermarked image and said associated verification key to a remote system, and said extracting step and said comparing step are performed in said remote system.

17. The method of claim 14, further comprising the step of compressing said captured image prior to said watermarking step, whereby said measured parameters are watermarked into said compressed image.

18. A method for verifying the authenticity of a captured image, said captured image being generated by an image capturing system having means for measuring a plurality of parameters associated with said captured image and means for watermarking said plurality of parameters within said captured image, said method comprising the steps of:

specifying at least one of said plurality of parameters to be measured and watermarked by said image capturing system;

capturing an image of a desired object with said image capturing system;

watermarking said captured image of said object with said specified parameters;

generating a corresponding verification key based on said watermarked parameters;

storing said watermarked image and said corresponding verification key;

retrieving said watermarked image and said corresponding verification key;

extracting from said watermarked image said watermarked parameters using said verification key;

comparing said extracted parameters with said specified parameters to determine if said extracted parameters match said specified parameters.

19. The method of claim 18, further comprising the step of recording said specified

parameters, wherein said recorded parameters are compared with said extracted parameters.

20. The method of claim 19, wherein said step of recording said specified parameters includes one of electronically recording said specified parameters with said captured image and manually recording said specified parameters associated with said captured image.

21. The method of claim 13, wherein the step of measuring a plurality of parameters associated with said captured image comprises receiving and recording object data from an object in an observed image frame when the image is generated, said object data comprising object identification information.

22. The method of claim 18, wherein said plurality of parameters to be measured and watermarked comprises user data that is automatically transmitted from a user and recorded when said image is captured, said user data comprising user identification information.